No. 17-2

In the Supreme Court of the United States

UNITED STATES OF AMERICA,
Petitioner,

v.

MICROSOFT CORPORATION,
Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF OF MEMBERS OF CONGRESS AS AMICI CURIAE IN SUPPORT OF RESPONDENT

MICHAEL E. BERN
Counsel of Record
RYAN C. GROVER
ADAM J. TUETKEN
NAYHA ARORA*
LATHAM & WATKINS LLP
555 11th Street, NW
Suite 1000
Washington, DC 20004
(202) 637-1021
michael.bern@lw.com

**Admitted to practice in Pennsylvania only. All work supervised by a member of the DC Bar.*

Counsel for Amici Curiae Members of Congress

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iii

INTEREST OF AMICI CURIAE 1

SUMMARY OF ARGUMENT 2

ARGUMENT 4

I. THE PRESUMPTION AGAINST EXTRATERRITORIALITY SERVES IMPORTANT ENDS, AND IT IS FOR CONGRESS, NOT COURTS, TO DEPART FROM IT 4

A. The Presumption Avoids Unintended International Conflict 5

B. Congress Alone Has The Authority And Ability To Craft Policies That Apply Extraterritorially 7

C. The Presumption Allows Congress To Legislate More Effectively 11

II. THE PRESUMPTION AGAINST EXTRATERRITORIALITY IS POWERFULLY IMPLICATED BY THIS CASE 12

A. The SCA's Text And Legislative History Underscore That Congress Neither Expected Nor Intended For The SCA To Be Applied Extraterritorially 13

B. The Seizure Of Data Stored Overseas Entails An Extraterritorial Application Of The SCA 19

TABLE OF CONTENTS—Continued

Page

1. Interpreting The SCA To Require The Transfer And Production Of Data Maintained Overseas Threatens International Discord 19
2. Congress Is Better Situated To Resolve Whether And When U.S. Warrant Procedures Should Apply To Data Stored Abroad 22
3. Interpreting The SCA To Apply To Data Stored Abroad Will Undermine The Benefits Of The Presumption Against Extraterritoriality In Future Cases 27

III. CONGRESS, RATHER THAN THE COURTS, IS THE APPROPRIATE BRANCH TO ADDRESS THE SCA'S LIMITED SCOPE 29

CONCLUSION 37

TABLE OF AUTHORITIES

Page(s)

CASES

American Banana Co. v. United Fruit Co.,
213 U.S. 347 (1909).....6

American Insurance Association v. Garamendi,
539 U.S. 396 (2003).....15

The Apollon, 22 U.S. (9 Wheat.) 362 (1824).....6

Benz v. Compania Naviera Hidalgo, S.A.,
353 U.S. 138 (1957).....4, 6, 9, 29, 30

Brown v. Duchesne,
60 U.S. (19 How.) 183 (1857).....30

Chicago & Southern Air Lines, Inc. v. Waterman Steamship Corp.,
333 U.S. 103 (1948).....8

Doe v. Drummond Co.,
782 F.3d 576 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 1168 (2016).....13

EEOC v. Arabian American Oil Co.,
499 U.S. 244 (1991).....*passim*

F. Hoffman-La Roche Ltd. v. Empagran S.A.,
542 U.S. 155 (2004).....7

FAA v. Cooper,
566 U.S. 284 (2012).....16

TABLE OF AUTHORITIES—Continued

Page(s)

Henson v. Santander Consumer USA, Inc.,
137 S. Ct. 1718 (2017).....29

Keller Foundation/Case Foundation v. Tracy,
696 F.3d 835 (9th Cir. 2012), *cert. denied*, 133 S. Ct. 2825 (2013).....14

Kiobel v. Royal Dutch Petroleum Co.,
569 U.S. 108 (2013).....2, 4, 6, 29

Loginovskaya v. Batratchenko,
764 F.3d 266 (2d Cir. 2014).....14

McCulloch v. Sociedad Nacional De Marineros De Honduras,
372 U.S. 10 (1963).....9

Molzof v. United States,
502 U.S. 301 (1992).....16

Morrison v. National Australia Bank Ltd.,
561 U.S. 247 (2010).....*passim*

Murray v. The Schooner Charming Betsy,
6 U.S. (2 Cranch) 64 (1804).....7

Oetjen v. Central Leather Co.,
246 U.S. 297 (1918).....8

Perry v. Merit Systems Protection Board,
137 S. Ct. 1975 (2017).....29

TABLE OF AUTHORITIES—Continued

Page(s)

Pfeiffer v. Wm. Wrigley Jr. Co.,
755 F.2d 554 (7th Cir. 1985).....10

RJR Nabisco, Inc. v. European Community,
136 S. Ct. 2090 (2016).....4, 5, 11, 28, 30

The Schooner Exch. v. McFaddon,
11 U.S. (7 Cranch) 116 (1812).....5

Smith v. United States,
507 U.S. 197 (1993).....4

Sosa v. Alvarez-Machain,
542 U.S. 692 (2004).....8

United States v. Yousef,
327 F.3d 56 (2d Cir.), *cert. denied*, 540
U.S. 933 (2003).....7

Vieth v. Jubelirer,
541 U.S. 267 (2004).....9

Zivotofsky v. Clinton,
566 U.S. 189 (2012).....9

STATUTES

18 U.S.C. § 2510(12).....14

18 U.S.C. §§ 2701-2712.....1

18 U.S.C. § 2703(a).....15

29 U.S.C. § 623(f)(1).....10

TABLE OF AUTHORITIES—Continued

Page(s)

29 U.S.C. § 630(f) 13

Pub. L. No. 111-79, 123 Stat. 2086 (2009) 18

LEGISLATIVE MATERIALS

92 Cong. Rec. S6809 (daily ed. June 18, 2009) 18

155 Cong. Rec. H10093 (daily ed. Sept. 30, 2009) 18

163 Cong. Rec. S3082 (daily ed. May 23, 2017) 17, 20, 26

H.R. 3718, 115th Cong. (2017) 33

H.R. Rep. No. 99-647 (1986) 15, 16

S. 1671, 115th Cong. (2017) 33, 34, 35

S. Rep. No. 98-467 (1984), *reprinted in* 1984 U.S.C.C.A.N. 2974 10

S. Rep. No. 99-541 (1986) 15, 16

OTHER AUTHORITIES

Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evoloving Security and Right Issues*, 8 J. Nat'l Sec. L. & Pol'y 473 (2016) ..... *passim*

TABLE OF AUTHORITIES—Continued

Page(s)

Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary, 115th Cong. (June 15, 2017, Bloomberg).....31, 32, 33

European Parliament, Parliamentary Questions, No. E-010602/2014 (last updated Mar. 10, 2015), http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-010602&language=EN 25

Senator Orrin G. Hatch, *Let's Pass the International Communications Privacy Act*, Remarks at BSA: The Software Alliance Event (Sept. 26, 2017).....17, 20, 32

Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders*, The Hague Inst. for Global Just., Conference on the Future of Cyber Governance (May 1, 2014), http://ssrn.com/abstract=2430275.....21

International Conflicts of Law and Their Implications for Cross Border Data Requests by Law Enforcement: Hearing before the H. Comm. on the Judiciary, 114th Cong. (2016).....20, 24, 25, 26

TABLE OF AUTHORITIES—Continued

Page(s)

Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 Penn. L. Rev. 373 (2014) 17

Vivek Krishnamurthy, *Cloudy with a Conflict of Laws*, Berkman Ctr. For Internet & Soc'y at Harvard Univ., Research Pub. No. 2016-3 (Feb. 16, 2016), https://dash.harvard.edu/bitstream/handle/1/28566279/SSRN-id2733350.pdf?sequence=1 25

Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary (Law Enforcement Access to Data Stored Across Borders Hearing), 115th Cong. (2017) ..... *passim*

Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights (Panel 1): Hearing Before the S. Comm. on the Judiciary, 115th Cong. (May 24, 2017, Bloomberg) 31, 33

Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights (Panel 2): Hearing Before the S. Comm. on the Judiciary, 115th Cong. (May 24, 2017, Bloomberg) 31

TABLE OF AUTHORITIES—Continued

Page(s)

U.S. House of Representatives Judiciary Comm., *Hearing: Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era* (June 15, 2017), https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era/.....9

INTEREST OF AMICI CURIAE[1]

Amici Curiae are members of the United States Senate and House of Representatives, who have introduced or co-sponsored the International Communications Privacy Act, bipartisan legislation currently under consideration by Congress which aims to establish a comprehensive framework to govern when and to what extent U.S. warrants may be used to access data stored abroad. *Amici* are therefore intimately familiar with the challenge and importance of effectively balancing the competing foreign policy, privacy, law enforcement, and economic interests that would be implicated by such a step.

Amici are also uniquely positioned to address the importance of the presumption against extraterritoriality and its application to this case. The presumption against extraterritoriality dictates that the choice of whether and to what extent U.S. law should apply beyond our nation's borders is reserved for Congress, not the courts. Congress has a strong institutional interest in the application of the presumption against extraterritoriality to statutes like the Stored Communications Act (SCA) (codified at 18 U.S.C. §§ 2701-2712) that Congress did not expect or intend to apply beyond the nation's borders.

---

[1] No counsel for a party authored this brief in whole or in part; and no such counsel or any party made a monetary contribution intended to fund the preparation or submission of this brief. No person or entity, other than *amici*, their members, and their counsel, made a monetary contribution intended to fund the preparation or submission of this brief. Petitioner and respondent have filed blanket consents to the filing of *amicus* briefs.

Amici appreciate that there are important practical consequences that follow from the faithful application of the presumption against extraterritoriality in this case. But such policy considerations are properly addressed by Congress through new legislation, not by twisting the SCA to apply in circumstances that Congress did not intend.

The members of Congress joining this brief are:

- Sen. Orrin Hatch (R-UT)
- Sen. Christopher Coons (D-DE)
- Rep. Doug Collins (R-GA)
- Rep. Darrell Issa (R-CA)
- Rep. Hakeem Jeffries (D-NY)

SUMMARY OF ARGUMENT

This Court has long recognized that Congress ordinarily intends for its acts to apply only within the territorial jurisdiction of the United States. That understanding is embodied in the "presumption against extraterritoriality"—an important canon of statutory construction intended to reserve to Congress, rather than the courts, the complex and consequential policy decision of whether and in what circumstances federal law should reach beyond the nation's borders. By directing that congressional acts shall be interpreted to reach no further than the territorial limits of the United States absent express indicia to the contrary, the presumption ensures that courts do not "erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches." *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 116 (2013).

The presumption against extraterritoriality requires affirmance in this case. Neither the text

nor history of Title II of the Electronic Communications Privacy Act (ECPA)—commonly referred to as the SCA—evinces any affirmative indication that Congress intended the Act to authorize the seizure of data stored within a foreign sovereign nation. The Solicitor General's claim that the presumption against extraterritoriality is not implicated by this case is misplaced. To the contrary, the principles underlying the presumption urge strongly against reading the SCA in a manner that Congress would not have anticipated and that would precipitate significant foreign policy consequences.

The Solicitor General also argues that the SCA should be interpreted to authorize the seizure of data stored outside the United States in order to avoid undermining law enforcement and national security interests. Those interests are undeniably important. But those policy considerations—all of which are the product of technological developments that significantly post-date the SCA's enactment—do not justify distorting the SCA to apply in circumstances that Congress neither considered nor intended. Congress, not this Court, is the appropriate branch to address the Solicitor General's concerns—through affirmative legislation. Indeed, there is growing bipartisan support within Congress for enacting a comprehensive framework to govern the circumstances in which a warrant may be utilized to secure access to data stored overseas. Whether and to what extent such a procedure should be authorized is a prerogative reserved to Congress. This Court should not undermine the important principles served by the presumption against extraterritoriality by twisting the SCA to apply in

this case—a step that could have dangerous repercussions not only in this case, but for future lawmaking.

ARGUMENT

I. THE PRESUMPTION AGAINST EXTRATERRITORIALITY SERVES IMPORTANT ENDS, AND IT IS FOR CONGRESS, NOT COURTS, TO DEPART FROM IT

"Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100 (2016). This presumption against extraterritoriality is a well-established canon of statutory construction and a "longstanding principle of American law." *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010) (quoting *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991) (*Aramco*)).

The presumption serves important separation of powers principles and protects against "unwarranted judicial interference in the conduct of foreign policy." *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 116 (2013). *First*, the presumption avoids unintended international conflicts that would result from applying U.S. law abroad where Congress has not so intended. *See id.* at 115. *Second*, the presumption reflects that Congress, not the courts, "alone has the facilities necessary to make fairly such an important policy decision" as whether and to what extent U.S. law should apply beyond our nation's borders. *Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957). *Third*, by setting forth a clear rule of interpretation that

accords with the "commonsense notion that Congress generally legislates with domestic concerns in mind," *Smith v. United States*, 507 U.S. 197, 204 n.5 (1993), the presumption allows Congress to legislate more effectively.

A. The Presumption Avoids Unintended International Conflict

As an initial matter, the presumption serves "to protect against unintended clashes between our laws and those of other nations." *Aramco*, 499 U.S. at 248. The presumption reflects the notion that Congress, not the courts, is best positioned to decide whether and to what extent American law should apply in ways that could (1) interfere with other nations' sovereignty, (2) lead to retaliation by foreign nations, and (3) precipitate conflicts with international law. The presumption "serves to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries" by ensuring that such conflicts are not triggered unless "Congress has *affirmatively and unmistakably* instructed" that a statute should reach outside the territory of the United States. *RJR Nabisco*, 136 S. Ct. at 2100 (emphasis added).

First, interpreting federal law to reach only the territorial jurisdiction of the United States absent express indication that Congress intended otherwise "avoid[s] unreasonable interference with other nations' sovereign authority." *Id.* at 2107 n.9. As Chief Justice Marshall explained, "[t]he jurisdiction of the nation within its own territory is necessarily exclusive and absolute. . . . Any restriction upon it, deriving validity from an external source, would imply a diminution of its sovereignty." *The Schooner*

Exch. v. McFaddon, 11 U.S. (7 Cranch) 116, 136 (1812). Ordinarily, therefore, applying one nation's law in the territory of another amounts to "an interference with the authority of another sovereign, contrary to the comity of nations, which the other state concerned justly might resent." *Am. Banana Co. v. United Fruit Co.*, 213 U.S. 347, 356 (1909). Such interference can have substantial consequences for the United States' relations with other countries and can trigger damaging friction with a foreign nation.

Second, the choice to apply the law of the United States to conduct abroad can lead foreign nations to retaliate by applying their law to conduct within the United States. *See, e.g.*, *Benz*, 353 U.S. at 147 (noting that the decision of whether to extend laws extraterritorially is "an important policy decision" because "retaliative action [is] so certain"). The presumption against extraterritoriality thus avoids judicial "interference in . . . a delicate field of international relations" that could result in retaliation by other nations, absent an "affirmative intention of the Congress clearly expressed." *Kiobel*, 569 U.S. at 115-16 (alteration in original) (quoting *Benz*, 353 U.S. at 147).

Third, extending U.S. law abroad risks precipitating unintended conflicts with international law. Congress generally intends for its legislation to comply with the law of nations. *Cf. The Apollon*, 22 U.S. (9 Wheat.) 362, 371 (1824) ("It would be monstrous to suppose that our revenue officers were authorized to enter into foreign ports and territories, for the purpose of seizing vessels which had offended against our laws. It cannot be presumed that Congress would voluntarily justify such a clear

violation of the laws of nations."). By guarding against constructions of U.S. law that conflict with international law, the presumption against extraterritoriality "helps the potentially conflicting laws of different nations work together in harmony—a harmony particularly needed in today's highly interdependent commercial world." *F. Hoffman-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164-65 (2004).

To be sure, "'Congress is not bound by international law,' [so] 'it may legislate with respect to conduct outside the United States, in excess of the limits posed by international law.'" *United States v. Yousef*, 327 F.3d 56, 86 (2d Cir.) (citations omitted), *cert. denied*, 540 U.S. 933 (2003). But the presumption against extraterritoriality ensures that that weighty decision is reserved for Congress, not the courts, to make in the first instance. Accordingly, the presumption provides that U.S. law is not to be construed to violate the law of nations absent an explicit and purposeful decision by Congress that compels that result. *Cf. Murray v. The Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804) ("[A]n act of Congress ought never to be construed to violate the law of nations if any other possible construction remains . . . .").

B. Congress Alone Has The Authority And Ability To Craft Policies That Apply Extraterritorially

The presumption also promotes the separation of powers by recognizing that Congress, rather than the courts, is endowed with the authority and capability to determine whether and to what extent U.S. law should apply outside the territory of the

United States. The Constitution purposefully gives responsibility for foreign policy to the political branches. *See Oetjen v. Cent. Leather Co.*, 246 U.S. 297, 302 (1918). The decisions involved in foreign policy "are delicate, complex, and involve large elements of prophecy," and therefore "should be undertaken only by those directly responsible to the people whose welfare they advance or imperil." *Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948). For that reason, this Court has candidly acknowledged that foreign policy involves "decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry." *Id.*; *see also Oetjen*, 246 U.S. at 302. Courts, therefore, should be "particularly wary of impinging on the discretion of the Legislative and Executive Branches in managing foreign affairs." *Sosa v. Alvarez-Machain*, 542 U.S. 692, 727 (2004).

As noted above, this Court has recognized that Congress "alone has the facilities necessary to make fairly such an important policy decision" as whether and how U.S. law should apply abroad "where the possibilities of international discord are so evident." *Benz*, 353 U.S. at 147. Unlike courts, Congress has the capacity to (a) work directly with foreign governments;[2] (b) discuss proposals with key

---

[2] *See, e.g.*, *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary (Law Enforcement Access to Data Stored Across Borders Hearing)*, 115th Cong. at 3 (May 10, 2017) (statement of Paddy McGuiness, United Kingdom Deputy National Security Adviser), https://www.judiciary.senate.gov/

domestic and foreign stakeholders, including businesses, policy organizations, executive officials, state officials, and diplomats;[3] and (c) tailor its decisions to the national security and foreign policy interests of the United States.[4] By contrast, a court can decide issues based only on legal arguments, from the parties at bar, confined by precedent. *See, e.g.*, *Zivotofsky v. Clinton*, 566 U.S. 189, 203 (2012) (Sotomayor, J., concurring in part and concurring in judgment) (""The judicial Power" created by Article III, § 1, of the Constitution is not *whatever* judges choose to do,' but rather the power 'to act in the manner traditional for English and American courts.'" (quoting *Vieth v. Jubelirer*, 541 U.S. 267, 278 (2004) (plurality opinion))). Because Congress can employ tools that the courts cannot, the presumption against extraterritoriality reinforces the principle that foreign policy "arguments should be directed to the Congress rather than to [the Court]." *McCulloch v. Sociedad Nacional De Marineros De Hond.*, 372 U.S. 10, 22 (1963).

---

imo/media/doc/05-24-17%20McGuinness%20Testimony.pdf (testifying that the United Kingdom intends to work closely with Congress on efforts to amend the SCA to facilitate a UK-US. Bilateral Agreement on Data Access).

[3] *See, e.g.*, U.S. House of Representatives Judiciary Comm., *Hearing: Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era* (June 15, 2017), https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era/ (listing witnesses).

[4] *See, e.g.*, *Law Enforcement Access to Data Stored Across Borders Hearing*, 115th Cong. at 10-14 (May 24, 2017) (statement of Brad Wiegmann, Deputy Assistant Att'y Gen. of the United States), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf (discussing foreign relations implications of amending the SCA).

Congress also is free to "calibrate its provisions in a way [the courts] cannot," *Aramco*, 499 U.S. at 259, including by tailoring the extraterritorial reach of a statute to reach conduct abroad only in certain circumstances. Congress is uniquely able, therefore, to avoid all-or-nothing propositions that fail to balance competing foreign policy and domestic considerations.

For instance, prior to 1984, courts applied the presumption against extraterritoriality to limit the reach of the Age Discrimination in Employment Act (ADEA) overseas. *See, e.g., Pfeiffer v. Wm. Wrigley Jr. Co.*, 755 F.2d 554, 557 (7th Cir. 1985) (addressing application of ADEA prior to 1984). In 1984, however, Congress amended the ADEA to reach some—but not all—conduct abroad. *Aramco*, 499 U.S. at 256. In so doing, "Congress specifically addressed potential conflicts with foreign law" by balancing domestic and foreign interests, *id.*—making explicit that "the amendment is carefully worded to apply only to citizens of the United States who are working for U.S. corporations or their subsidiaries," S. Rep. No. 98-467, at 27 (1984), *reprinted in* 1984 U.S.C.C.A.N. 2974, 3000), and permitting employers to take actions inconsistent with the ADEA when "compliance with [the ADEA] would cause such employer . . . to violate the laws of the country in which such workplace is located," *Aramco*, 499 U.S. at 256 (quoting 29 U.S.C. § 623(f)(1)).

Faithful application of the presumption against extraterritoriality in that case—as in others—permitted Congress to legislate the kind of balanced result that a court could not. *See, e.g., Pfeiffer*, 755 F.2d at 557 (noting the court could find no

"principled basis for confining the extraterritorial reach of the statute" to specified circumstances prior to 1984 in order to minimize foreign complications). That outcome promoted separation of powers principles by leaving to Congress the authority to craft a framework that appropriately accounted for the various competing concerns at issue.

C. The Presumption Allows Congress To Legislate More Effectively

Finally, the presumption against extraterritoriality "preserv[es] a stable background against which Congress can legislate with predictable effects." *Morrison*, 561 U.S. at 261. When courts presume that Congress legislates domestically, Congress need not contemplate the foreign consequences of every piece of legislation. Instead, it may legislate with confidence that its acts will not be interpreted to apply extraterritorially absent express indicia to the contrary. *See Aramco*, 499 U.S. at 258 (listing statutes that showed "Congress' awareness of the need to make a clear statement that a statute applies overseas"); *see id.* at 256 ("It is also reasonable to conclude that had Congress intended Title VII to apply overseas, it would have addressed the subject of conflicts with foreign laws and procedures.").

Legislating extraterritorially is a challenging task that courts should not lightly assume Congress undertook. "The presumption . . . aims to distinguish instances in which Congress consciously designed a statute to reach beyond U.S. borders, from those in which nothing plainly signals that Congress directed extraterritorial application." *RJR Nabisco*, 136 S. Ct. at 2112 (Ginsburg, J., concurring

in part and dissenting in part). The presumption provides a stable background rule, therefore, that promotes effective and purposeful lawmaking by Congress and consistent interpretation by courts.

As this Court has recognized, failures by courts in other cases to apply the presumption faithfully has "produced a collection of tests for divining what Congress would have wanted, complex in formulation and unpredictable in application." *Morrison*, 561 U.S. at 255-56. That uncertain world has made it difficult at times for Congress to legislate and increased the risk of mistaken interpretation by courts. Fidelity to the presumption, by contrast, promotes certainty and accuracy by affording both the legislative and judicial branch a clear rule to guide the formation and construction of legislative acts.

II. THE PRESUMPTION AGAINST EXTRATERRITORIALITY IS POWERFULLY IMPLICATED BY THIS CASE

Both the text and legislative history of the SCA establish that Congress did not intend or expect the SCA to authorize the seizure of data held within the territory of a foreign, sovereign nation. Consistent with the presumption against extraterritoriality, therefore, the SCA should not be construed to permit the seizure at issue in this case.

The Solicitor General argues that interpreting the SCA to authorize the forced disclosure of data stored abroad does not violate the presumption against extraterritoriality. This is mistaken. The principles underlying the presumption underscore that interpreting the SCA to authorize warrants to seize documents stored within a foreign country

would amount to an extraterritorial application of the statute.

A. The SCA's Text And Legislative History Underscore That Congress Neither Expected Nor Intended For The SCA To Be Applied Extraterritorially

This Court has reiterated that "[w]hen a statute gives no clear indication" of an intent that the statute have "extraterritorial application, it has none." *Morrison*, 561 U.S. at 255. Here, nothing in the text or legislative history of the SCA evinces a clear congressional intent for the statute to apply to data located outside the United States. To the contrary, the SCA's language and structure strongly support that Congress did not intend for the SCA to apply extraterritorially.

1. To begin with, the text of the SCA does not contain any of the sorts of provisions or definitions one would expect to find if Congress intended the law to apply extraterritorially. *See, e.g., Aramco*, 499 U.S. at 258-59 (Congressional intent to apply ADEA overseas clear where statute was amended to apply to "any individual who is a citizen of the United States employed by an employer in a workplace in a foreign country" (quoting 29 U.S.C. § 630(f))); *see also Doe v. Drummond Co.*, 782 F.3d 576, 601-02 (11th Cir. 2015) (holding that actions can be brought under 28 U.S.C. §§ 1331, 1350 for conduct occurring abroad because the text of the statute "provides for the liability of any individual who acts 'under actual or apparent authority, or color of law, *of any foreign nation*'" (emphasis added in original) (citation omitted)), *cert. denied*, 136 S. Ct. 1168 (2016).

Instead, the SCA is silent with respect to whether and to what extent its warrant procedure should apply to electronic documents stored on foreign soil. *See* Pet. App. 21a. "[T]he traditional principle" is that "silence means no extraterritorial application." *Morrison*, 561 U.S. at 260-61; *see, e.g.*, *Loginovskaya v. Batratchenko*, 764 F.3d 266, 271 (2d Cir. 2014) (concluding that the private right of action under the Commodity Exchange Act (CEA) does not apply to extraterritorial commodities transactions because "[t]he CEA as a whole . . . is silent to extraterritorial reach"); *Keller Found./Case Found. v. Tracy*, 696 F.3d 835, 845-47 (9th Cir. 2012) (concluding that Congress's application of 33 U.S.C. § 903(a) to the "navigable waters of the United States" does not include "foreign territorial waters and their adjoining ports and shore-based areas" because there was no indication Congress envisioned extraterritorial application), *cert. denied*, 133 S. Ct. 2825 (2013).

Moreover, the statute contains *affirmative* indicia that Congress did not intend the statute to apply extraterritorially. The SCA is part of ECPA, and thus subject to ECPA's definitions. Those definitions, in turn, evince an intent to exclude extraterritorial activity. ECPA defines an electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). As the legislative history makes clear, the phrase "that affects interstate or foreign commerce" in this definition was "not intend[ed] . . . [to] regulate activities

conducted outside of the territorial United States." H.R. Rep. No. 99-647, at 32 (1986); *see* S. Rep. No. 99-541, at 12 (1986).

The fact that Congress empowered state and local law enforcement officers to invoke the SCA, and authorized state courts to issue warrants under the Act's provisions, is further indication that Congress did not intend the SCA to operate overseas. *See* 18 U.S.C. § 2703(a) (providing that State warrant procedures are an adequate basis for issuance of an SCA warrant); Pet. App. 25a. Congress does not lightly devolve authority to state courts to take actions that could and would conflict with foreign laws and procedures. *See Am. Ins. Ass'n v. Garamendi*, 539 U.S. 396, 413 (2003) (noting "the 'concern for uniformity in this country's dealings with foreign nations' that animated the Constitution's allocation of the foreign relations power to the National Government in the first place" (citation omitted)). In particular, Congress would not provide for such far-reaching state court authority without at least "address[ing] the subject of conflicts with foreign laws and procedures." *Aramco*, 499 U.S. at 256.

Finally, Congress's use of the term "warrant," rather than "subpoena," in the SCA should not be lightly dismissed. The government relies heavily on the "backdrop of settled law about the execution of subpoenas," Pet. Br. 32-40, in arguing that warrants under the SCA should reach documents stored in other countries. But Congress should be taken to mean what it said when it chose to use the term "warrant"—a well-understood word that carries territorial limitations. As this Court has rightly noted, "when Congress employs a term of art,"

Congress "'presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken.'" *FAA v. Cooper*, 566 U.S. 284, 292 (2012) (quoting *Molzof v. United States*, 502 U.S. 301, 307 (1992)).

2. The SCA's legislative history likewise supports the conclusion that Congress was concerned with regulating access to data held domestically, not with creating a procedure to seize information located within the sovereign territory of a foreign nation.

ECPA, of which the SCA was a principal part, was designed to address the technological advances of the *1980s*. Congress passed ECPA in 1986 to update existing federal wiretap laws to protect the privacy of data transmitted through new methods of electronic communication. S. Rep. No. 99-541, at 1 (1986). These new methods of communication included electronic mail, computer-to-computer communication, cellular and cordless telephones, paging devices, remote computing devices, and computerized recordkeeping systems. H.R. Rep. No. 99-647, at 22-23 (1986); S. Rep. No. 99-541, at 2, 8-10. The SCA was designed to regulate "access to stored wire and electronic communications" in order "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." S. Rep. No. 99-541, at 3, 12.

The prospect of transnational data access and storage would have been inconceivable to the statute's drafters, who neither foresaw nor sought to address such a state of affairs. While the SCA addressed the cutting-edge technologies of its time, the differences between the technology of 1986 and

modern cloud computing underscore that Congress understandably did not envision that the SCA would apply to data abroad. In 1986, when the SCA was enacted, data was typically stored on users' personal computers or on local servers. 163 Cong. Rec. S3082 (daily ed. May 23, 2017) (statement of Sen. Hatch); *see also* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 Penn. L. Rev. 373, 391, 404, (2014) (stating that storage costs in the 1980s were so high that email communications were "typically" downloaded to personal computers and deleted from servers, "[f]ew sent communications were saved," and communication over computers "occurred mostly in the United States"). Consistent with the technological limitations of its time, nothing in the SCA—or its accompanying legislative history—refers to transnational data storage, retrieval of electronic data stored in other countries, or related jurisdictional conflicts.

U.S. service providers *now* serve customers around the world, including billions of foreign citizens—a state of affairs that was inconceivable in 1986. And service providers *today* use cloud and remote network computing to store electronic data on servers across the globe to improve efficiency, increase the speed of delivery, reduce energy costs, and lower tax rates. *See Law Enforcement Access to Data Stored Across Borders Hearing*, 115th Cong. at 2 (May 24, 2017), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Daskal%20Testimony.pdf (statement of Jennifer Daskal, Associate Professor, American University Washington College of Law). But Congress did not have any of these issues in mind when it enacted the SCA in 1986. *See* Senator Orrin G. Hatch, *Let's Pass the International*

Communications Privacy Act at 1, Remarks at BSA: The Software Alliance Event (Sept. 26, 2017) (on file with author) (stating that today's rapid movement of data across borders "was never within Congress's contemplation" when the SCA was enacted).

Subsequent amendments to ECPA reinforce that Congress did not understand or intend for the SCA to reach information stored abroad. In 2009, Congress enacted the Foreign Evidence Request Efficiency Act, Pub. L. No. 111-79, 123 Stat. 2086 (2009). That act was intended to streamline requests by foreign governments for assistance in reaching communications within the United States in order to, among other things, promote reciprocal treatment of U.S. requests for data stored in other countries. *See, e.g.*, 155 Cong. Rec. H10093-94 (daily ed. Sept. 30, 2009); 92 Cong. Rec. S6809-10 (daily ed. June 18, 2009). The need for an amendment to prompt better reciprocal access for U.S. officials to data stored abroad is further indication that Congress—even as late as 2009—did not understand the SCA to apply to such data of its own force.

Both the SCA's text and legislative history demonstrate that Congress did not expect the SCA to apply to data stored outside the United States. Accordingly, the presumption against extraterritoriality dictates that the SCA should not be construed to reach beyond our nation's borders.

B. The Seizure Of Data Stored Overseas Entails An Extraterritorial Application Of The SCA

The Solicitor General argues that invoking the SCA to obtain data outside the United States does not implicate extraterritoriality at all, and therefore does not violate the presumption against extraterritoriality. Pet. Br. 18-32. That is mistaken. All of the principal justifications underlying the presumption are fully implicated by the question of whether a congressional statute should be construed to authorize the seizure of electronic documents stored on foreign soil. Construing the SCA to apply to data stored in facilities located abroad could trigger international conflict and encourage foreign nations to retaliate in ways that would harm U.S. privacy and law enforcement interests. It would extend U.S. law abroad notwithstanding that Congress did not expect that result, nor even weigh its costs and benefits. And it would undermine the stability of a pivotal background rule against which Congress legislates, introducing uncertainty that would impose long-term institutional costs on both Congress and courts.

1. Interpreting The SCA To Require The Transfer And Production Of Data Maintained Overseas Threatens International Discord

Interpreting the SCA to require the transfer and production of data maintained overseas—in many cases involving data of foreign citizens—would precipitate precisely the kind of international discord and retaliation that the presumption against extraterritoriality is intended to avoid.

a. Governments have a substantial interest in applying their own data disclosure and privacy laws to their own citizens, as well as to data located within their borders. *See* 163 Cong. Rec. at S3082 (statement of Sen. Hatch). When the United States unilaterally applies U.S. warrants extraterritorially to compel the disclosure of such data, it may frustrate those interests and violate foreign laws. *See* Senator Hatch, *supra*, at 1; *International Conflicts of Law and Their Implications for Cross Border Data Requests by Law Enforcement: Hearing before the H. Comm. on the Judiciary (International Conflicts of Law Hearing)*, 114th Cong. 50-52 (2016) (statements of Rep. Ken Buck). This type of affront to state sovereignty risks sowing distrust and creating discord with foreign allies and foes. *International Conflicts of Law Hearing*, 114th Cong. 52 (statement of Rep. Ken Buck)

b. Interpreting the SCA to permit unilateral action abroad and to require companies to seize information located within other foreign nations also invites retaliation in kind, thereby jeopardizing the important national interest in protecting the privacy of U.S. citizens and their data.

To begin with, the use of the SCA prior to and outside of this case to gather data abroad has emboldened other nations to seek or demand similar access to data stored in the United States. Foreign nations—hostile and friendly alike—are interested in accessing data stored in the United States to meet critical law enforcement needs. *See id.* at 12 (statement of David Bitkower, Principal Deputy Assis ant Attorney General, Criminal Division, Department of Justice); *Law Enforcement Access to Data Stored Across Borders Hearing*, 115th Cong.

at 6-8, https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, Department of Justice). As the holder of the "lion's share of the world's data," the United States is of particular interest to law enforcement agencies throughout the world. *See* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evoloving Security and Right Issues*, 8 J. Nat'l Sec. L. & Pol'y 473, 485 (2016).

It is well recognized that the United States plays "an outsized role" in driving standards for data access, such that its approach here "is likely to become a model for other[] [nations]." *Id.* at 474. Compelling the disclosure of data stored abroad would thus encourage foreign countries to respond in kind and pursue unfettered access to data located in the United States. *Law Enforcement Access to Data Stored Across Borders Hearing*, 115th Cong. at 7-8 (May 10, 2017), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Smith%20Testimony.PDF (statement of Brad Smith, President & Chief Legal Officer, Microsoft Corporation). That result would undermine the important national interest in protecting the privacy of information generated by U.S. citizens or stored in the United States. *Id.*

Foreign nations also may retaliate by enacting legislation designed to thwart international access to data located within their own territory. Indeed, many foreign governments—fearing access by U.S. law enforcement to data held by U.S. providers abroad—have instituted data localization laws or otherwise attempted to hide their data from the United States. Daskal, *supra*, at 476-79; Jonah

Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders*, The Hague Inst. for Global Just., Conference on the Future of Cyber Governance 5-6 (May 1, 2014), http://ssrn.com/abstract=2430275. Data localization laws seek to keep data within a country's control by requiring providers to store and process data locally, or by favoring providers that are incorporated or that maintain principal places of business in that country. Daskal, *supra*, at 476-77. In addition to making it more difficult for U.S. law enforcement to access data held abroad, such laws also jeopardize the economic benefits and efficiencies that cloud computing creates for consumers and harm U.S. companies at the forefront of the multibillion dollar cloud industry.

This is precisely the kind of case, therefore, in which the presumption against extraterritoriality is particularly warranted—to avoid the international discord and retaliation that would result from construing a statute to reach abroad in a manner that Congress neither expected nor intended.

2. Congress Is Better Situated To Resolve Whether And When U.S. Warrant Procedures Should Apply To Data Stored Abroad

When Congress legislates in areas in which there are rapidly evolving conditions—like technology—*Congress*, rather than the judiciary, is the branch responsible for monitoring and updating the law to respond to changing conditions. The question, therefore, of whether and when U.S. law enforcement should be authorized to compel access

to data stored abroad is a policy decision best left to Congress. Only Congress has the constitutional authority and capacity to craft a framework for accessing information held abroad that balances America's foreign policy interests with privacy concerns, public safety needs, and business interests.

a. The decision of whether and when a federally authorized warrant procedure may be used to obtain information located abroad implicates numerous competing policy interests in addition to foreign policy.

i. *Public Safety.* Law enforcement agencies rely on electronic communications data, including emails and text messages, to investigate and thwart crimes. *See Law Enforcement Access to Data Stored Across Borders Hearing*, 115th Cong. at 1 (statement of B. Wiegmann) (stating that "[t]he need for effective, efficient, and lawful access to data in criminal investigations is paramount in the digital age"). Any comprehensive framework governing the use of warrants overseas must be sensitive to the needs of law enforcement in promoting public safety.

At the same time, the needs of law enforcement are not necessarily best served by "allow[ing] the government free rein to demand communications, wherever located, from any service provider, of whatever nationality, relating to any customer, whatever his or her citizenship or residence, whenever it can establish probable cause to believe that those communications contain evidence of a violation of American criminal law, of whatever degree of seriousness." Pet. App. 69a. Indeed, the construction of the SCA advanced by the Solicitor General is likely to prove counterproductive by inciting foreign nations to enact data localization

laws that would diminish U.S. access to data abroad. *See Law Enforcement Access to Data Stored Across Borders Hearing*, 115th Cong. at 7-8 (statement of B. Wiegmann); *see also International Conflicts of Law Hearing*, 114th Cong. 27 (statement of David Bitkower, Principal Deputy Assistant Attorney General, Criminal Division, Department of Justice).

ii. *Privacy.* In today's interconnected world, the privacy of data created and stored by U.S. citizens and permanent residents is directly impacted by whether and to what extent the United States authorizes the seizure of data stored abroad. Authorizing access to data held abroad increases the likelihood that foreign governments will retaliate by seeking access to data held within the United States, thereby jeopardizing the privacy interests of U.S. citizens and companies. That concern is particularly acute because some other countries are far less protective of privacy interests than the United States when instituting compulsory process.

Conflicting legal regimes concerning data privacy and disclosure also encourage other countries to rely on domestic law enforcement procedures and even clandestine methods to circumvent foreign laws in order to acquire data located abroad. *See* Daskal, *supra*, at 490. Such a free-for-all would undercut the privacy interests of U.S. citizens and companies by making it difficult to regulate access to data and enforce even a minimum standard of privacy on the Internet. *See id.*

iii. *Business And Consumer Interests.* Requiring U.S. service providers to remove data from a foreign country can expose U.S. service providers to conflicting legal obligations and increased costs, and render international data

storage less efficient and more expensive for consumers.

Foreign governments often make direct requests to service providers—including the local subsidiaries of foreign companies—to disclose data that those providers possess. *See International Conflicts of Law Hearing*, 114th Cong. 2 (statement of Rep. Bob Goodlatte); Vivek Krishnamurthy, *Cloudy with a Conflict of Laws*, Berkman Ctr. For Internet & Soc'y at Harvard Univ., Research Pub. No. 2016-3 (Feb. 16, 2016), https://dash.harvard.edu/bitstream/handle/1/28566279/SSRN-id2733350.pdf?sequence=1. Service providers that receive such requests may find themselves ensnared in a web of conflicting data privacy laws promulgated by multiple governments, each claiming jurisdiction over the same data. In such instances, providers are forced to choose which law to follow, which can lead to unpredictable results for law enforcement and backlash against providers, thereby harming U.S. business interests and competitiveness. *See* Daskal, *supra*, at 490.

This case is illustrative. The United States issued a warrant requesting data from Microsoft that was stored on a server in Ireland. Ireland is a member of the European Union (EU), and in response to the facts of this case, the European Commission has stated that EU law does not permit foreign governments to access data in the EU through providers and instead requires that such requests be submitted to the relevant government. *See* European Parliament, Parliamentary Questions, No. E-010602/2014 (last updated Mar. 10, 2015), http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-010602&language=EN. If the SCA is construed to apply to the data at issue in this

case, compliance with one law could require Microsoft to violate the other. That scenario places U.S. providers at risk of violating foreign laws and incurring penalties. *See, e.g.*, 163 Cong. Rec. at S3082 (statement of Sen. Hatch).[5]

These competing legal obligations also translate to increased costs for businesses and consumers. Foreign data localization laws enacted in retaliation for extraterritorial application of U.S. law may push U.S. providers out of foreign markets or force them to build additional data centers in foreign countries. *See Law Enforcement Access to Data Stored Across Borders Hearing*, 115th Cong. at 1-2 (statement of B. Smith). These laws also threaten to fragment the Internet and limit providers' ability to store data in the most cost-effective and efficient manner. *See* Daskal, *supra*, at 473.

b. Left unresolved, the conflicting international legal landscape governing data disclosure is likely to lead to suboptimal policy outcomes. On the one hand, governments could continue passing laws to impede foreign access to data housed within their borders. *See id.* at 490. Such a fractious and contentious legal landscape would limit providers' capacity to efficiently store data, as well as law enforcement's ability to gather it. *Id.* at 473, 491. On the other hand, governments could continue

---

5 In spring 2018, the EU General Data Protection Regulation is scheduled to take effect. That law would restrict the U.S. Government from requesting data unilaterally from EU providers and instead channel such requests through the relevant government. Service providers will violate this law if they disclose data in response to U.S. warrants. *International Conflicts of Law Hearing*, 114th Cong. 63-64 (statement of Brad Smith, President & Chief Legal Officer, Microsoft Corporation).

seeking unconstrained access to data anywhere in the world. *Id.* Allowing such unregulated access, especially to countries with weak privacy regimes or nefarious objectives, would imperil user privacy across the Internet. *See id.*

Reconciling the competing policy interests at stake in transnational data access requires delicate policy determinations that are appropriately left to Congress. This is precisely the kind of case in which application of the presumption against extraterritoriality serves separation of powers principles by ensuring that the complex and inherently policy-driven decision of whether to apply U.S. law abroad is left to the branch with the constitutional authority and capacity to make that decision.

3. Interpreting The SCA To Apply To Data Stored Abroad Will Undermine The Benefits Of The Presumption Against Extraterritoriality In Future Cases

Amici can testify to the valuable role played by the presumption against extraterritoriality in promoting effective lawmaking by Congress, as well as ensuring predictable interpretation of those laws by courts. To construe the SCA to authorize the seizure of data stored abroad would seriously undermine that sense of surety as Congress legislates and courts interpret laws going forward.

The presumption against extraterritoriality is intended to "preserv[e] a stable background against which Congress can legislate with predictable effects." *Morrison*, 561 U.S. at 261. It promotes effective lawmaking by freeing Congress from having

to anticipate the potential foreign consequences of every legislative decision and by providing clear guidance to courts regarding how to interpret congressional acts that are silent with respect to extraterritorial application. Interpreting the SCA to apply to data stored outside the United States would frustrate both of these goals.

The Solicitor General argues that the "focus" of the SCA's warrant procedure is domestic even in situations where the data is seized from within a foreign nation, because it results in "the disclosure of electronic records to the government *in the United States*." Pet. Br. 13 (emphasis added). That does not pass muster. Applying the SCA to data stored abroad would authorize the compelled seizure of electronic documents and data stored within a foreign country and the removal of that information to the United States. To comply with the warrant, some person, machine, or process in the foreign country would have to access the data and transmit it back to the United States—conduct all "focus[ed]" outside the territory of the United States. *RJR Nabisco*, 136 S. Ct. at 2101. Though the technology involved is more sophisticated, the effect is identical to a statute that authorized the government to serve a warrant requiring an individual in the United States to travel to a foreign country, remove documents or other physical evidence from foreign soil, and then turn that data over to law enforcement in the United States.

If the presumption against extraterritoriality is held not to apply here, notwithstanding that a contrary construction would authorize direct impacts outside the United States and trigger important implications for foreign relations, it will introduce

substantial uncertainty for both lawmakers and courts. Congress will be forced to parse proposed legislation to anticipate future cases in which its words might be construed to authorize or proscribe conduct outside the United States that is difficult or even impossible to foresee at the time of the law's passage. And courts are likely to reach less predictable results, increasing the risk of judicial "interference in . . . a delicate field of international relations" and outcomes that Congress did not consider or intend. *Kiobel*, 569 U.S. at 115-16 (alteration in original) (quoting *Benz*, 353 U.S. at 147). Such a result is both deeply problematic and unwarranted by the facts of this case.

III. CONGRESS, RATHER THAN THE COURTS, IS THE APPROPRIATE BRANCH TO ADDRESS THE SCA'S LIMITED SCOPE

The Solicitor General argues that limiting the SCA to apply to data stored outside the territory of the United States would lead to deleterious policy consequences by "hamper[ing] domestic law enforcement and counterterrorism efforts." Pet. Br. 41-45. No one disputes the importance of those policy considerations. But those concerns cannot and do not justify departing from the presumption against extraterritoriality in this case. "[T]he proper role of the judiciary" is "to apply, not amend, the work of the People's representatives." *Henson v. Santander Consumer USA, Inc.*, 137 S. Ct. 1718, 1726 (2017). And "the business of enacting statutory fixes [is] one that belongs to Congress and not this Court." *Perry v. Merit Sys. Prot. Bd.*, 137 S. Ct. 1975, 1988 (2017) (Gorsuch, J., dissenting). The concerns identified by the Solicitor General are

appropriately addressed not by distorting the SCA, but by congressional action.

Indeed, Congress is currently working to do just that. There is bipartisan support for enacting a revised framework to govern access to data stored abroad that aims to carefully balance competing policy considerations and set forth comprehensive and clear rules. This Court need not and should not, therefore, "strain[] [the scope of the SCA] to reach cases which Congress evidently could not have contemplated." *Benz*, 353 U.S. at 146 n.7 (quoting *Brown v. Duchesne*, 60 U.S. (19 How.) 183, 197 (1857)).

1. The Solicitor General argues that this Court should interpret the SCA to reach data stored abroad to avoid "serious administrability concerns" that the Solicitor General says could hinder domestic law enforcement and counterterrorism efforts. Pet. Br. 41. But the question before this Court is not to evaluate "whether . . . 'Congress would have wanted' a statute to apply to foreign conduct 'if it had thought of the situation before the court,' but whether Congress has affirmatively and unmistakably instructed that the statute will do so." *RJR Nabisco*, 136 S. Ct. at 2100 (citation omitted). As discussed *supra* at 13-18, Congress did not do that here.

The Solicitor General insists that the "real-world consequences" that would follow from interpreting the SCA not to apply to data stored abroad "further suggest that Congress did not adopt the scheme that Microsoft proposes." Pet. Br. 41. But the asserted consequences on which the Solicitor General relies are entirely the product of technological developments over the last three decades. Because

those developments were not before Congress in 1986, they provide no basis to interpret the SCA in a manner inconsistent with the presumption against extraterritoriality.

2. Few disagree that the SCA should be updated to meet the demands of today's modern world. But the appropriate branch to address that problem is Congress, not the judiciary.

a. Members of both houses of Congress—and both parties—recognize that the "[c]urrent legal framework . . . is insufficient for addressing the needs of the technology and the society of the 21st Century." *Data Stored Abroad: Ensuring Lawful Access and Pr. acy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (June 15, 2017, Bloomberg) (June 2017 *Data Stored Abroad Hearing*) (statement of Rep. Tom Marino). Indeed, there is general appreciation that the SCA'a current structure is "a mismatch between old law and new technology." *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights (Panel 2): Hearing Before the S. Comm. on the Judiciary*, 115th Cong. (May 24, 2017, Bloomberg) (statement of Prof. Jennifer Daskal). As a result, members of Congress recognize that "[a] legislative fix to the Stored Communications Act is necessary to remedy the problem made clear by the *Microsoft* decision." June 2017 *Data Stored Abroad Hearing*, 115th Cong. (June 15, 2017, Bloomberg) (statement of Rep. Robert Goodlatte). Members further agree that Congress "has a key role to play by promptly passing the legislative fixes necessary." *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights*

(Panel 1): Hearing Before the S. Comm. on the Judiciary, 115th Cong. (May 24, 2017, Bloomberg) (*Panel 1 Law Enforcement Access to Data Stored Across Borders Hearing*) (statement of Sen. Sheldon Whitehouse).

b. In crafting a response to the demands of modern technology, Congress is free to "calibrate its provisions in a way that [the courts] cannot," *Aramco*, 499 U.S. at 259. As Judge Lynch noted below, neither the interpretation of the SCA advanced by the Solicitor General nor the interpretation put forward by respondents is sufficient to balance the competing foreign policy, privacy, law enforcement, and economic interests implicated by the question presented in this case. Pet. App. 68a-69a. Unlike courts, however, Congress has the authority and capability to balance those concerns and "need not make an all-or-nothing choice." *Id.* at 69a.

Members of Congress, including *amici*, are thus actively working on crafting a solution to update the SCA to "ensure that law enforcement has the tools it needs to solve crime . . . while also protecting the privacy of our fellow citizens . . . in a way that does not create international conflicts or place U.S. providers at risk of violating foreign law." Senator Hatch, *supra*, at 1.

Congress appreciates that updating the SCA necessitates the enactment of "a comprehensive framework that takes into account our very global, interconnected economy and at the same time balances our many needs." June 2017 *Data Stored Abroad Hearing* (statement of Rep. Pramila Jayapal). "[S]imply reversing the Second Circuit" is inadequate to address those concerns. *Id.*

(statement of Rep. John Conyers). Rather, reform requires "find[ing] a process that will accommodate the . . . needs of the business community[,] . . . our national security needs, and [the] needs of law enforcement." *Panel 1 Law Enforcement Access to Data Stored Across Borders Hearing* (statement of Sen. Lindsey Graham). Congress is uniquely and exclusively authorized by the Constitution to undertake that task.

3. Congress is working in bipartisan fashion to fulfill that constitutional responsibility. The International Communications Privacy Act (ICPA) (S. 1671, 115th Cong. (2017)) exemplifies that effort. ICPA is sponsored in the Senate by Republican Senator Orrin Hatch and co-sponsored by Democratic Senator Christopher Coons and Republican Senator Dean Heller. In the House of Representatives, a companion bill (H.R. 3718, 115th Cong. (2017)) has been introduced by Republican Representative Doug Collins and co-sponsored by Republican Representative Darrell Issa and Democratic Representatives Hakeem Jeffries and Suzan DelBene.

ICPA is designed to balance the "many interests that must be recognized when law enforcement agencies seek information from providers," including "the legitimate needs of law enforcement agencies in the United States," "the privacy interests of all customers," and "the legitimate interests of governments to protect the human rights, civil liberties and privacy of their nationals and residents." S. 1671 § 2(3)(A)-(C). ICPA balances these interests first by clarifying that the government can compel disclosure of "the contents of a wire or electronic communication that is stored,

held, or maintained by the provider . . . *only pursuant to a warrant* issued using the procedures described in the Federal Rules of Criminal Procedure" or in accordance with state law. *Id.* § 3(a)(2)(A) (emphasis added). ICPA then authorizes the government to compel disclosure of data stored outside the United States in certain circumstances. *See id.* § 3(a)(3) (proposed 18 U.S.C. § 2703A(a)(1)) But it also provides that disclosure may not be required in situations where the individual whose data is sought is neither a U.S. citizen, lawful permanent resident, nor physically located within the United States. *Id.* § 3 (proposed 18 U.S.C. § 2703A(d)(2)(A)).

Because extraterritorial application of U.S. law can create conflict with foreign law, ICPA balances the need for U.S. law enforcement agencies to obtain communications of non-U.S. persons with the importance of avoiding offense to foreign countries. To ensure that warrant applications are made in good faith, ICPA requires applications to "state the nationality and location of the subscriber or customer whose communications are being sought, unless the nationality and location cannot reasonably be determined." *Id.* § 3(a)(2)(D). And when nationality and location cannot be determined, ICPA directs that the application must state "the investigative steps" taken to make the determination. *Id.*

ICPA likewise seeks to avoid offense to foreign nations by creating a new Section 2703A that governs warrants to individuals located outside the United States who are nationals of "qualifying foreign countries." *Id.* § 3(a)(3). ICPA accounts for the sovereignty interests of foreign countries by

requiring that "qualifying foreign countries" receive notice of the warrant application and an opportunity to object before the warrant will issue. *Id.* § 3(a)(3) (proposed 18 U.S.C. § 2703A(a)(1)). But ICPA avoids unnecessary foreign entanglements by limiting objections to situations in which disclosure would violate the "qualifying foreign country's" laws. *Id.* (proposed 18 U.S.C. § 2703A(c)). If an objection occurs, ICPA instructs courts to undertake a comity analysis to determine whether the foreign country's interests should prevail over law enforcement's interest in disclosure. This balance accounts for the important interests implicated when U.S. businesses operating outside the United States encounter conflicting legal obligations. It also provides clear guidance on how companies should handle such conflicts.

ICPA balances these interests without sacrificing the United States' national security interests or its role as a leader on the world stage. ICPA shortens the objection period to 7 days in cases of exigency or physical danger, and provides that notice to the qualifying foreign country may be delayed for up to 90 days where there is reason to believe that disclosure would jeopardize an investigation or national security. *Id.* § 3(a)(3) (proposed 18 U.S.C. § 2703A(d)(1)(A), (2)(A)(i)). Instead of retaliation, ICPA encourages reciprocity. In order to be a "qualifying foreign country," a foreign nation must meet certain privacy and international human rights standards and provide reciprocal access to U.S. law enforcement agencies to data stored within its borders. *See id.* (proposed 18 U.S.C. § 2703A(e)(1)(B)).

4. That Congress did not engage in a similar balancing effort regarding access to data stored abroad when enacting the SCA is powerful evidence that Congress did not intend for the SCA to reach such information. Addressing the consequences of that choice from three decades ago is a task for Congress, not the courts. This Court should not twist the SCA to apply in a manner in which it was neither expected nor intended to do. Rather, this Court should leave it to Congress to enact legislation, such as ICPA, that carefully balances the competing interests implicated by compelling access to data stored overseas.

Construing the SCA to apply to data held overseas, by contrast, not only would precipitate international discord and jeopardize weighty privacy and economic interests, but it would also augur significant negative consequences for Congress's future lawmaking. Congress depends on the presumption against extraterritoriality to avoid unintended consequences and to have confidence concerning when and where its laws will be applied. This Court should not and need not depart from the presumption in this case, but instead should permit Congress to complete its efforts to resolve the complex problems presented by this case in the manner—and forum—contemplated by the Constitution.

CONCLUSION

For the foregoing reasons, the judgment of the court of appeals should be affirmed.

Respectfully submitted,

MICHAEL E. BERN
Counsel of Record
RYAN C. GROVER
ADAM J. TUETKEN
NAYHA ARORA*
LATHAM & WATKINS LLP
555 11th Street, NW
Suite 1000
Washington, DC 20004
(202) 637-1021
michael.bern@lw.com

**Admitted to practice in Pennsylvania only. All work supervised by a member of the DC Bar.*

Counsel for Amici Curiae Members of Congress

JANUARY 18, 2018